Леонид Н. Кессаринский[1], Алексей С. Артамонов[2], Фарид Ф. Тайибов[2],
Кирилл А. Коваль[1], Анна С. Каменева[2], Дмитрий В. Бойченко[2], Грайр А. Овсепян[3]
[1]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
e-mail: LNKessarinskiy@mephi.ru, https://orcid.org/0000-0001-7756-6166
e-mail: Kirilloid53@yandex.ru, https://orcid.org/0000-0003-3296-0340
[2]АО «ЭНПО СПЭЛС»,
Каширское ш., 31, г. Москва, 115409, Россия
e-mail: Asart@spels.ru, https://orcid.org/0000-0002-5158-8292
e-mail: Fftai@spels.ru, https://orcid.org/0000-0002-0370-4180
e-mail: ASPih@spels.ru, https://orcid.org/0000-0002-0735-937X
e-mail: Dvboy@spels.ru, https://orcid.org/0000-0002-8382-4675
[3]National Instruments,
ул. Овсепа Эмина, д. 123, г. Ереван, 0051, Армения
e-mail: hrayr.hovsepyan@ni.com, https://orcid.org/0000-0002-5273-3025

ИДЕНТИФИКАЦИЯ ЭЛЕМЕНТНОЙ КОМПОНЕНТНОЙ БАЗЫ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

DOI: http://dx.doi.org/10.26583/bit.2018.3.07

Аннотация. Одним из основных направлений обеспечения безопасности киберфизических систем является создание и внедрение технологий гарантированно устойчивых к различным видам внешних воздействий. Ключевым аспектом создания таких устойчивых технических устройств является применение в разработках стойкой к внешним воздействующим факторам (ВВФ) элементной компонентной базы (ЭКБ). Актуальность данной проблемы определяется в частности ростом доли контрафактной продукции в электронике как международного тренда, определяющего необходимость идентифицировать изделия, предназначенные для ответственных применений. Помимо выявления контрафакта идентификация изделий элементной компонентной базы необходима для достоверной и информативной оценки стойкости к внешним воздействующим факторам. Одна из основных задач методики оценки стойкости - установить эффективный баланс между достоверностью результатов тестирования и трудоемкостью процедуры. Трудности оптимизации заключены в основном в количестве разрушенных образцов, необходимом объеме собираемой информации, обеспечении выявления контрафакта. В работе представлена эффективная процедура идентификации, совмещающая «разрушающие» и «неразрушающие» виды проверок, выявление контрафакта, неоднородности выборки, подозрительных изделий. Усовершенствована процедура идентификации образцов выборок для проведения испытаний. Приведены примеры экспериментально выявленных случаев контрафакта. Показана необходимость идентификации для обеспечения достоверности и информативности результатов испытаний. Также приведены дополнительные преимущества от получаемой в ходе процедуры информации при оптимальной реализации.

Ключевые слова: безопасность, идентификация, киберфизические системы, контрафакт, элементная компонентная база.

Для цитирования: КЕССАРИНСКИЙ, Леонид Н. et al. ИДЕНТИФИКАЦИЯ ЭЛЕМЕНТНОЙ КОМПОНЕНТНОЙ БАЗЫ КИБЕРФИЗИЧЕСКИХ СИСТЕМ. Безопасность информационных технологий, [S.l.], n. 3, p. 67-78, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1141>. Дата доступа: 28 aug. 2018. doi:http://dx.doi.org/10.26583/bit.2018.3.07.

Leonid N. Kessarinskiy[1], Alexey S. Artamonov[2], Farid F. Taibov[2], Kirill A. Koval[1],
Anna S. Kameneva[2], Dmitriy V. Boychenko[2], Hrair A. Hovsepyan[3]
[1]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoye shosse, 31, 115409, Moscow, Russia
e-mail: LNKessarinskiy@mephi.ru, https://orcid.org/0000-0001-7756-6166
e-mail: Kirilloid53@yandex.ru, https://orcid.org/0000-0003-3296-0340
[2]JSC ENPO SPELS,
Kashirskoye shosse, 31, 115409, Moscow, Russia
e-mail: Asart@spels.ru, https://orcid.org/0000-0002-5158-8292
e-mail: Fftai@spels.ru, https://orcid.org/0000-0002-0370-4180
e-mail: ASPih@spels.ru, https://orcid.org/0000-0002-0735-937X

e-mail: Dvboy@spels.ru, https://orcid.org/0000-0002-8382-4675
[3]National Instruments
Hovsep Emin street, 123, Yerevan, 0051, Armenia
e-mail: hrayr.hovsepyan@ni.com, https://orcid.org/0000-0002-5273-3025

Authentication of electronics components for cyber-physical systems

DOI: http://dx.doi.org/10.26583/bit.2018.3.07

Abstract. One of the main directions of cyber-physical systems safety ensuring is the creation and implementation of technologies for providing the electronics components a resistance to various types of external influences. The relevance of this problem is the increase of a rate of counterfeit products in electronics as an international trend. This determines a need to authenticate the products intended for responsible applications. In addition to the issue of counterfeit, the electronics components authentication is necessary for a reliable and informative assessment of their resistance to the impacts from external factors. One of the main tasks of the methodology for assessing the resistance is to establish an effective optimal balance between the reliability of the test results and the procedure laboriousness. The difficulties of this optimization are related mainly to the number of destroyed samples, the volume of collected information, ensuring of a counterfeit identification. Hereby we present an effective authentication procedure combining the "destructive" and "non-destructive" types of checks with the counterfeit identification, sample heterogeneity, and suspicious items. Improvement of the sampling procedure for testing is presented as well. The experimental results of authentication are discussed.
Keywords: information security, authentication, cyber-physical systems, counterfeit, electronics components.
For citation: KESSARINSKIY, Leonid N. et al. Authentication of electronics components for cyber-physical systems. IT Security (Russia), [S.l.], n. 3, p. 67-78, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1141>. Date accessed: 28 aug. 2018. doi:http://dx.doi.org/10.26583/bit.2018.3.07.

Введение

Современные технологические прорывы в области инфокоммуникационного обеспечения управления сложными системами привели к появлению относительно новых аспектов информационной безопасности, таких как «промышленная кибербезопасность» [1], безопасность интернета вещей [2], входящих в проблематику обеспечения безопасности киберфизических систем и имеющих свои особенности в отличие от проблемы защиты информации в «офисных» системах управления. Традиционная парадигма информационной безопасности, заключенная в триаде обеспечения доступности, целостности и конфиденциальности информации в этих случаях слабо применима. Более целесообразным, на наш взгляд, является представление об информационной безопасности как об обеспечении устойчивости системы управления, которое широко применяется в банковской сфере и интерпретируется как «обеспечение непрерывности бизнеса» [3].

Как подчеркнуто в новой редакции «Доктрины информационной безопасности Российской Федерации», утвержденной 5 декабря 2016 г. Президентом РФ, одним из основных направлений обеспечения безопасности критических систем управления является создание и внедрение технологий гарантированно устойчивых к различным видам внешних дестабилизирующих воздействий. Существенной угрозой потери устойчивости функционирования, в частности киберфизических систем, является общий мировой тренд роста контрафактной продукции в области микроэлектроники и электронных устройств на их основе, что приводит к неожиданным отказам критичных жизненно важных устройств, изделий для ответственных применений [4-6]. Поэтому с учетом приведенного выше представления о безопасности киберфизических систем становится очевидным, что ключевым фактором создания подобных устойчивых технических устройств является применение в разработках стойкой к внешним воздействующим факторам (ВВФ) элементной компонентной базы (ЭКБ) [7].

Оценка соответствия изделий ЭКБ требованиям по стойкости к ВВФ опирается на экспериментальные (в ходе испытаний) или расчетно-экспериментальные (на основе

анализа ранее полученных результатов испытаний изделий-аналогов) методы в соответствии с действующей нормативной базой (НД).

Одними из наиболее информативных и ответственных являются так называемые разрушающие испытания, например, радиационные, в результате которых образцы могут утратить работоспособное состояние. При этом возникает актуальная задача по обеспечению достоверности и информативности распространения результатов разрушающих испытаний ограниченной выборки образцов на всю сертифицируемую партию изделий ЭКБ [8-10].

В соответствии с действующей НД, описанная задача обеспечения достоверности оценки достигается необходимыми свойствами испытательной выборки, наиболее важными из которых являются:

- образцы испытываемой выборки должны выбираться из общей партии случайным образом;
- все образцы выборки должны быть однородными, т.е. принадлежать одной партии изготовления, иметь одинаковый внешний вид, одинаковые маркировки корпуса и кристаллов;
- маркировки корпуса должны быть нанесены промышленным способом, и внешний вид должен соответствовать шаблону из официальной документации;
- маркировка внутренних элементов изделия (например, кристаллов) должна соответствовать официальной документации.

Поэтому непосредственному процессу любых испытаний ЭКБ должна предшествовать обязательная процедура идентификации образцов выборки, которая удовлетворяет перечисленным выше условиям.

В настоящей работе приведены экспериментальные результаты исследований различных видов ЭКБ, показывающих актуальность поставленной выше задачи и доказывающих необходимость пристального внимания к ее решению.

Причиной отрицательного результата идентификации может быть выявленная неоднородность образцов выборки, несоответствие образцов (всех или части) официальной документации по маркировкам, внешнему виду и т.д. В этом случае, в зависимости от конкретных выявленных обстоятельств, могут быть приняты решения либо о разбиении выборки образцов на подвыборки (по принципу однородности), либо о недопуске всех образцов к сертификации как подозрительных и/или несоответствующих заявленному типу.

В различных испытательных центрах (ИЦ) процесс идентификации выборок ЭКБ регламентирован внутренними документами, имеет свои ограничения и учитывает специфику изделий, включенных в область аккредитации [7, 11-18]. Использованные в данной работе процедуры идентификации разработаны и постоянно совершенствуются в интересах госкорпорации «Роскосмос», госкорпорации «Росатом», а также организаций и предприятий Минпромторга России. Их эффективность подтверждена заключением ведущей экспертной организации по вопросам радиационных испытаний – Института экстремальной прикладной электроники НИЯУ МИФИ (ИЭПЭ НИЯУ МИФИ) и специалистами системы добровольной сертификации «Электронсерт» (см. [10]).

Процедура идентификации

Процедура идентификации состоит из процедуры «неразрушающего» и «разрушающего» контроля и интегрирована в общий процесс проведения исследований/испытаний. Основные этапы проведения идентификации кратко описаны ниже и далее проиллюстрированы примерами.

До проведения испытаний идентификация выполняется с применением «неразрушающих» методов контроля.

На первом этапе проверяется сопутствующая документация, официальное описание (с официального сайта): сведения о стране-изготовителе, типе корпуса, способе и шаблоне

маркировки партии, даты производства, стране-изготовителе, технологии, материале активной области, диапазоне рабочих температур. Пример сравнения показа на рис. 1.

Далее выполняется визуальный анализ внешнего вида корпусов и маркировок всех образцов одной партии (проверка образцов на идентичность). Образцы фотографируются сверху и снизу, затем сравнивается внешний вид изделия с данными из спецификации производителя.

После анализа внешнего вида проводится рентгеноскопия всех образцов одной партии. Основная задача рентгенографического контроля - проверка схем на идентичность по их внутренней структуре.

Также рентгеноскопия позволяет:

а) выявить и локализовать дефекты печатных плат и ИС, если они имеются;

б) определить размеры, местонахождение, количество и ориентацию кристаллов в полупроводниковых приборах и ИС;

в) определить расстояние от поверхности корпуса ИС до кристалла и волосков, соединяющих кристалл с контактами ИС (это необходимо для последующей декапсуляции микросхем, в том числе и для декапсуляции с сохранением работоспособности изделия).

Если все схемы одной выборки однородны, их допускают к проведению дальнейших испытаний. В противном случае отдельные схемы одной выборки с отличной структурой либо не испытывают, либо испытывают, предварительно учитывая выявленные различия.

После проведения испытаний процесс идентификации продолжается с использованием «разрушающих» методов идентификации.

Проводится декапсуляция изделий - удаление элементов корпуса для получения прямого визуального доступа к отдельным компонентам сборки и кристаллам, что позволяет достоверно идентифицировать образцы, поступившие на испытания.

В зависимости от типа корпуса декапсуляция микросхем проводится механически (керамика, металл, пластик с заполнением компаундом), лазерной резкой (пластик) или методом химического травления (пластик).

Полностью вскрытый (оголённый) кристалл фотографируется: сначала общий вид, затем маркировки на кристалле (под микроскопом).

Далее выполняется визуальный анализ текущих фотографий самих изделий, их рентгеновских снимков и фотографий кристалла со снимками однотипных изделий, поступавших в испытательный центр ранее.

По результатам идентификации пополняется база данных и выпускается протокол идентификации.

Примеры экспериментальных исследований

Поскольку радиационные разрушающие испытания являются в большинстве НД последним видом испытаний ЭКБ, для их проведения предназначаются выборки образцов уже успешно прошедших идентификацию на этапе предыдущих «неразрушающих» испытаний, например: на стойкость к механическим или климатическим воздействующим факторам, проверки параметров при крайних значениях рабочих температур среды и др.

Тем не менее при использовании описанной выше процедуры идентификации регулярно выявляется несоответствие представленных образцов требованиям к испытательным выборкам, в результате чего образцы не допускаются к проведению радиационных испытаний или допускаются с ограничениями. Далее представлены характерные типовые случаи негодных или подозрительных образцов.

1. Неоднородность выборки образцов для испытаний (по размеру кристалла)

Проведена идентификация выборки для испытаний из 17 образцов (№№ 18..34) микросхем XC95216 (*из соображений конфиденциальности полное название не приводится*) ф. Xilinx – программируемые логические интегральные схемы (ПЛИС) [16].

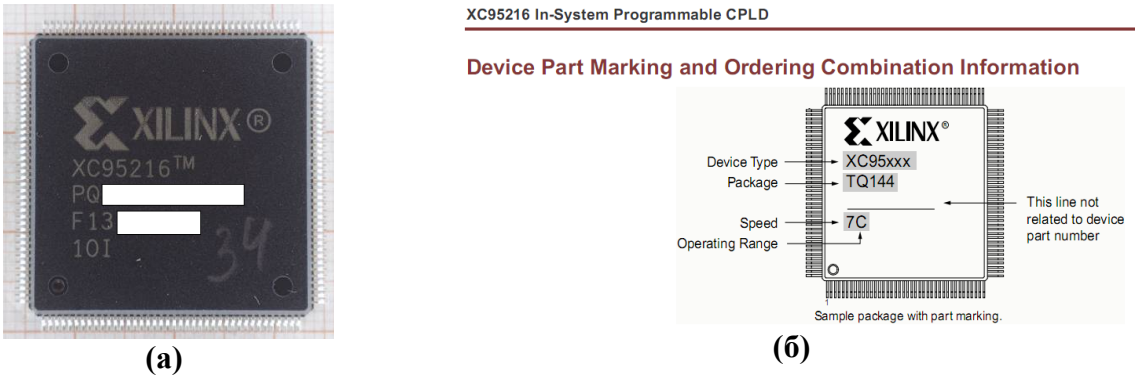
В результате визуального анализа идентичности установлено: все образцы имеют идентичную маркировку корпуса, логотипа, идентичное расположение метки ключа на корпусе и зон маркировок корпуса в соответствии с примером внешней маркировки официальной документации производителя. Сравнение образца выборки и примера маркировки из спецификации показано на рис. 1.

В результате рентгеновского анализа идентичности установлено: 16 образцов №№ 18..28, 30..34 имеют кристалл размером 7,8 х 6,5 мм; 1 образец № 29 имеет кристалл размером 10,1 х 12,0 мм. Результаты рентгеновского анализа приведены на рис. 2. Согласно поиску по базе данных ИЦ размеры кристалла однотипного изделия, ранее прошедшего испытания, составляли 7,7 х 6,4 мм.

Таким образом, неразрушающими методами идентификации была выявлена неоднородность выборки.

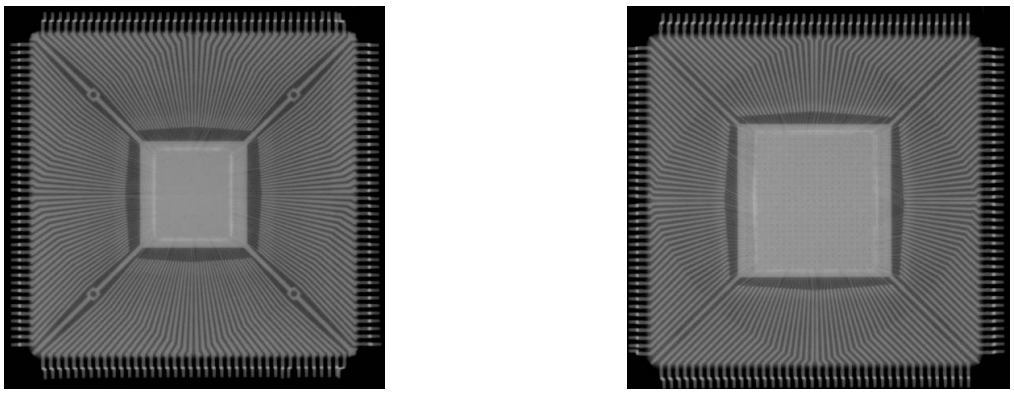
Для уточнения результатов анализа был проведен анализ маркировок кристаллов после декапсуляции образца выборки. На рис. 3 показаны фотографии кристалла. Метки совпали с метками ранее прошедшего испытания изделия.

Таким образом, из выборки микросхем XC95216 *(из соображений конфиденциальности полное название не приводится)* образец № 29 был исключен, остальные образцы были допущены к испытаниям.



(а) **(б)**

Рис. 1. Сравнение фотографии образцов XC95216 с маркировкой корпуса:
(а) – вид корпуса сверху (из соображений конфиденциальности полное название, дата изготовления и номер партии закрыты), (б) – маркировка из спецификации
(Fig. 1. Comparison photographs of the samples XC95216-marked case:
(a) – top view of the enclosure (for reasons of confidentiality, the full name, date of manufacture and batch number are closed), (b) - specification markings)



(а) (б)

Рис. 2. Рентгеновские фотографии образца XC95216:
(а) – вид корпуса сверху образец № 18 (как пример образцов №№ 18..28, 30..34),
(б) – вид корпуса сверху (образец № 29)
(Fig. 2. X-ray photo of the samples XC95216:
(a) – top view of sample № 18 (as an example of samples group №№ 18..28, 30..34),
(b) – top view of sample № 29 (different sample))

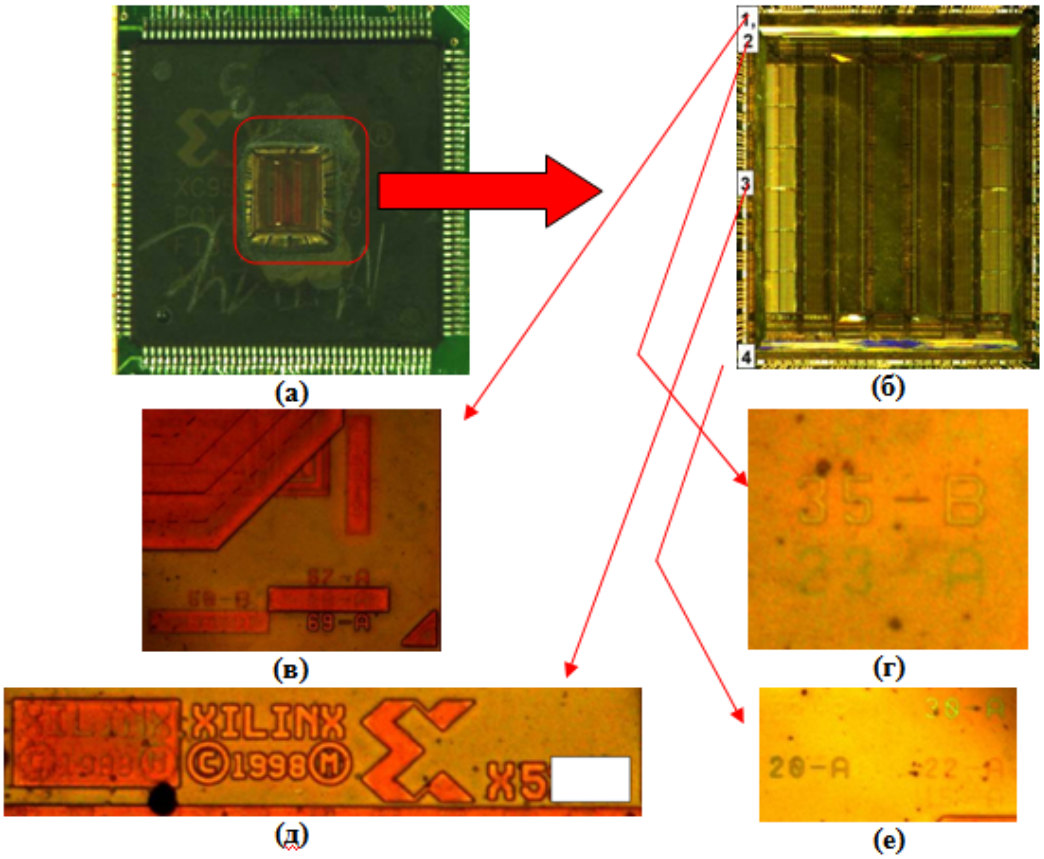


Рис. 3. Фотографии вскрытого образца №23 XC95216:
(а) – вид корпуса сверху, (б) – вид кристалла (цифрами 1…4 обозначены зоны маркировки), (в) – зона маркировки 1, (г) – зона маркировки 2, (д) – зона маркировки 3 (из соображений конфиденциальности полная маркировка закрыта), (е) – зона маркировки 4
(Fig. 3. Decapsulated sample № 23 XC95216 photo:
(a) – top view, (b) – chip photo (digits 1..4 are mark zones), (c) – mark zone 1, (d) – mark zone 2, (e) mark zone 3 (for reasons of confidentiality, the full mark is closed), (f) – mark zone 4)

2. Неоднородность выборки образцов для испытаний (по конструкции корпуса и размерам кристалла)

Проведена идентификация выборки для испытаний из 6 образцов мощных диодов Шоттки 30BQ040TR (*из соображений конфиденциальности полное название не приводится*) ф. Vishay Semiconductors.

В результате визуального анализа установлена однородность маркировок, соответствие маркировок (smd код компнента) официальной документации.

На этапе рентгеновского анализа выборки была выявлена неоднородность по критерию разной конструкции корпуса и размерам кристалла. На рис. 4 приведен рентгеновский снимок образцов выборки [20].

Таким образом, выборка образцов 30BQ040TR была разбита на две подвыборки, испытанные отдельно друг от друга. Информация о неоднородности выборки была передана заказчику испытаний.

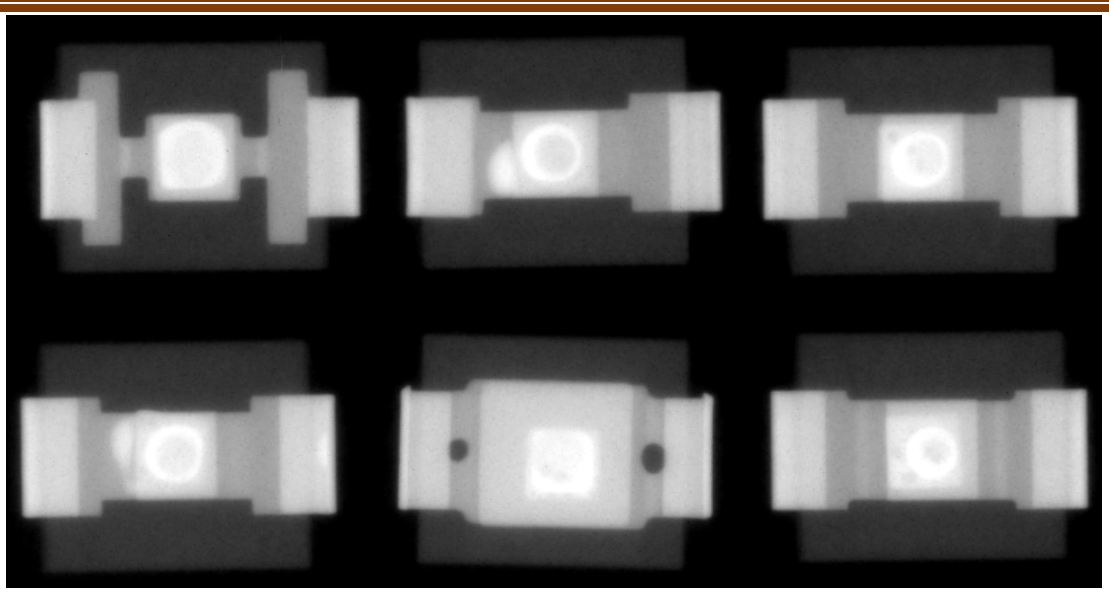


Рис. 4. Рентгеновская фотография выборки из 6 образцов 30BQ040TR: средний образец в нижнем ряду отличается по конструкции корпуса и размеру кристалла от остальных 5 образцов. (Fig. 4. X-ray photo of 6 samples 30BQ040TR group:middle bottom sample is the different one)

3. Неоднородность выборки образцов для испытаний (по конструкции корпуса)

Проведена идентификация выборки образцов микросхемы Am79C (*из соображений конфиденциальности полное название не приводится*) ф. Advanced Micro Devices – приемопередатчик стандарта Ethernet.

Визуальный анализ маркировок образцов не выявил неоднородность, но на этапе рентгеновской фотографии выделены две подвыборки образцов с разной конструкцией корпусов – показано на рис. 5.

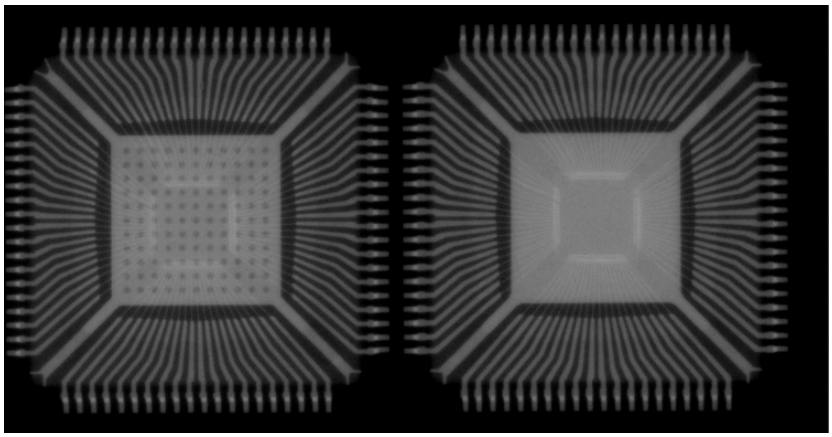


Рис. 5. Рентгеновская фотография образцов Am79C (из соображений конфиденциальности полное название не приводится): разная конструкция теплоотвода корпуса от кристалла. (Fig. 5. X-ray photo of samples Am79C (for reasons of confidentiality, the full name is closed): heat radiators have different constructions)

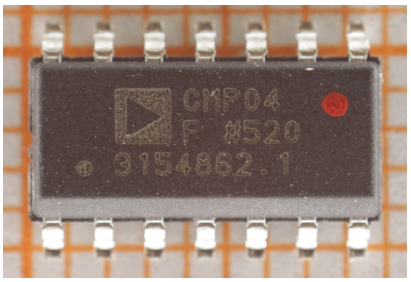
4. Однородность кристаллов образцов разных выборок и партий изготовления

Проведена идентификация трех выборок (разных лет испытаний) образцов микросхем CMP04 ф. Analog Devices – счетверенный аналоговый компаратор напряжений.

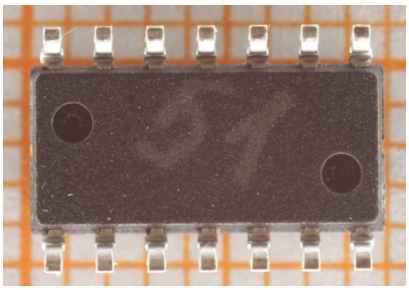
Результаты визуального анализа маркировок установили разные партии изготовления образцов трех выборок – фотографии приведены на рис. 6 [21].

В результате сравнения маркировок кристаллов образцов трех выборок установлена идентичность кристаллов. На рис. 7 приведены фотографии маркировок кристаллов трех выборок.

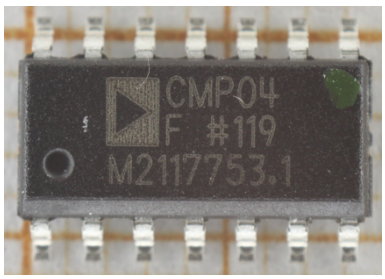
Таким образом, установлена идентичность кристаллов образцов разных выборок, и результаты испытаний прошлых лет распространены на образцы более новых выборок, т.е. оценка радиационной стойкости проведена расчетно-экспериментальный методом без испытаний.



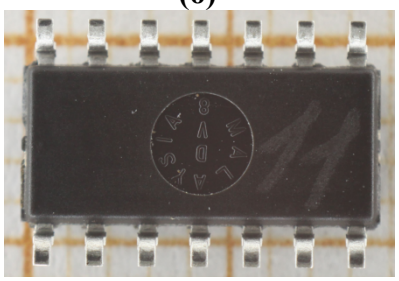
(а)



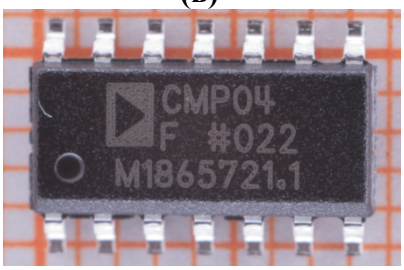
(б)



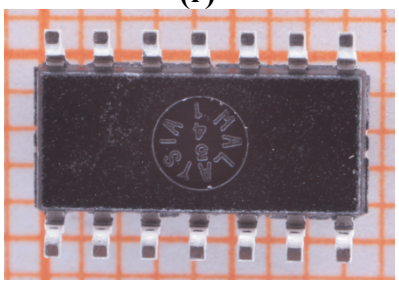
(в)



(г)

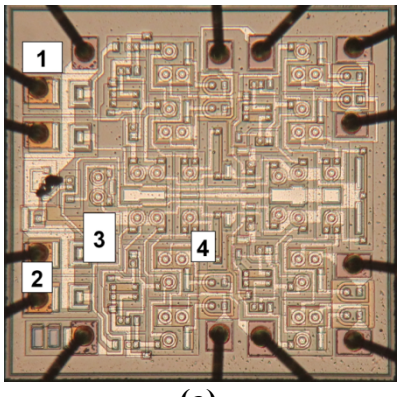


(д)

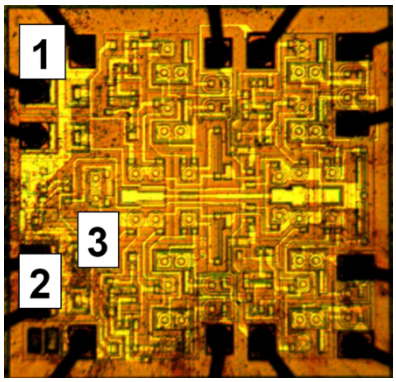


(е)

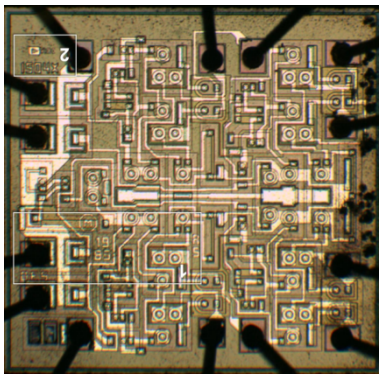
Рис. 6. Фотографии образцов трех выборок (попарно) микросхем CMP04
(Fig. 6. Photos of 3 group (by pair) CMP04 samples)



(а)



(б)



(в)

(г) **(д)** (е)

Рис. 7. Сравнение фотографий образца CMP04 и однотипных изделий после вскрытия корпуса
(Fig. 7. Comparison photos of CMP04 chip and the same types chips)

5. Подозрение на брак или контрафакт

Иногда в результате проведения идентификации выборок образцов выявляются огрехи производства, подозрение на бракованное изделие, неаккуратность корпусирования ЭКБ. Ниже несколько примеров таких результатов.

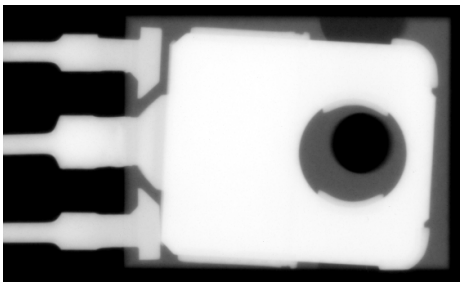


Рис. 8. Рентгеновская фотография смещенного расположения теплоотвода (радиатора) внутри пластикового корпуса мощного МОП транзистора IRG4PC40 ф. International Rectifier – 1 образец из выборки
(Fig. 8. X-ray photo of uneven heat radiator location in power MOS transistor package IRG4PC40 (International Rectifier) - 1 sample of group)

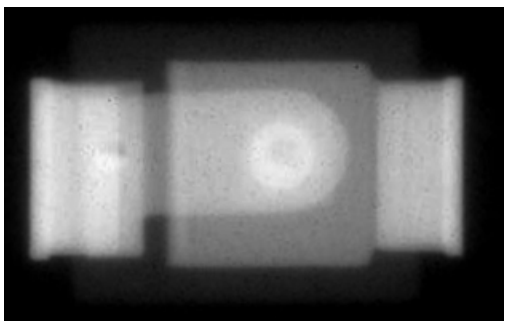


Рис. 9. Кривое взаимное расположение контактов и внутренних площадок корпуса чип-диода Шоттки 10BQ040 ф. Vishay Semiconductor
(Fig. 9. X-ray photo of uneven pins and inner package areas smd Schottky diode 10BQ040 (Vishay Semiconductor))

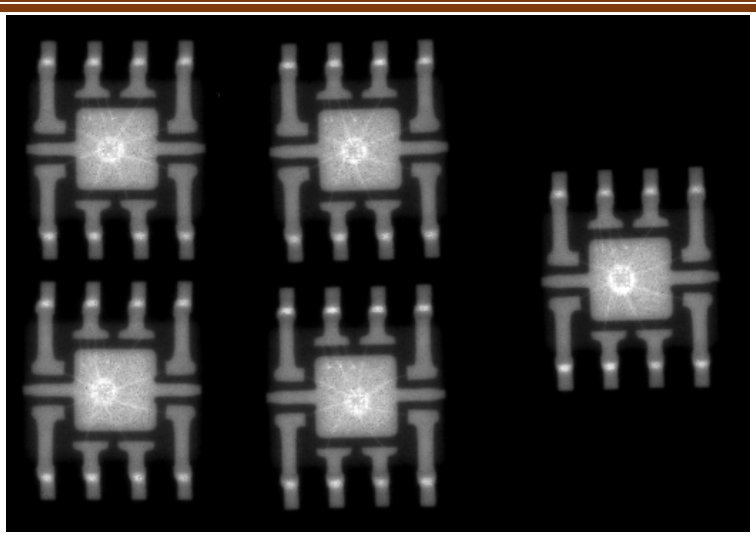


Рис. 10. Произвольное неотцентрованное расположение кристалла на площадке-теплоотводе корпуса микросхемы линейного стабилизатора напряжения MC13143D ф. Motorola (Fig. 10. The chaotic chip location in MC13143D (Motorola) package)

Заключение

Таким образом, приведенные данные экспериментальных исследований ЭКБ показывают актуальность процедур идентификации образцов выборок для разрушаюших испытаний, что приводит к выводу о необходимости включении таких процедур в различные системы оценки соответствия киберфизических систем по требованиям безопасности в качестве обязательного этапа технологии проведения испытаний для обеспечения информативности и достоверности результатов. При научном подходе разработки методов идентификации, её результаты являются дополнительным ценным источником информации, дающим реальное сокращение производственных затрат за счет исключения избыточных испытаний в том числе заведомо негодных образцов.

СПИСОК ЛИТЕРАТУРЫ:

1. Касперский, Е. В. В ЗАЛОЖНИКАХ У АВТОМАТИКИ: КАК ЗАЩИТИТЬ ПРОМЫШЛЕННОСТЬ ОТ КИБЕРАТАК. Безопасность информационных технологий, [S.l.], v. 23, n. 3, p. 7-10, oct. 2016. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/12>. Дата доступа: 11 july 2018.
2. Астье, Жан Ив; Жуков, Игорь Юрьевич; Мурашов, Олег Николаевич. СИСТЕМЫ УПРАВЛЕНИЯ «УМНЫЙ ДОМ» И ИНТЕРНЕТ ВЕЩЕЙ. Безопасность информационных технологий, [S.l.], v. 24, n. 3, p. 18-29, july 2017. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/260>. Дата доступа: 11 july 2018. doi:http://dx.doi.org/10.26583/bit.2017.3.02.
3. Егоров, Борис Михайлович et al. Основные направления обеспечения непрерывности функционирования информационно-телекоммуникационных систем высокой доступности. Безопасность информационных технологий, [S.l.], v. 21, n. 4, dec. 2014. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/137>. Дата доступа: 11 july 2018
4. Koushanfar, F., Fazzari, S., McCants, C., Bryson, W., Sale, M., Song, P., & Potkonjak, M. (2012). Can EDA combat the rise of electronic counterfeiting? Paper presented at the Proceedings - Design Automation Conference, 133-138. doi:10.1145/2228360.2228386 Retrieved from www.scopus.com
5. Alkabani, Y., Koushanfar, F., Kiyavash, N., & Potkonjak, M. (2008). Trusted integrated circuits: A nondestructive hidden characteristics extraction approach doi:10.1007/978-3-540-88961-8-8 Retrieved from www.scopus.com
6. Gassend, B., Lim, D., Clarke, D., Van Dijk, M., & Devadas, S. (2004). Identification and authentication of integrated circuits. Concurrency Computation Practice and Experience, 16(11), 1077-1098. doi:10.1002/cpe.805
7. Никифоров А. Ю. Развитие базовой технологии прогнозирования, оценки и контроля радиационной стойкости изделий микроэлектроники/Никифоров А. Ю., Скоробогатов П. К., Стриханов М. Н., Телец В. А., Чумаков А. И.//Известия высших учебных заведений. Электроника, 2012. -№ 5 (97). -С. 18-23.
8. Pope, S. (2008). Trusted integrated circuit strategy. IEEE Transactions on Components and Packaging Technologies, 31(1), 230-234. doi:10.1109/TCAPT.2008.918319

9. Ожегин Ю.А., Никифоров А. Ю, Телец В. А., Уваркин Д. С., Пыхтина А. С. Направления развития системы управления качеством радиационных испытаний электронной компонентной базы. Спецтехника и связь. 2011. № 4-5. С. 59-62.
10. Никифоров А. Ю., Телец В. А. Радиационная стойкость электронной компонентной базы систем специальной техники и связи//Спецтехника и связь, выпуск № 4-5, 2011.
11. Lofstrom, K., Daasch, W. R., & Taylor, D. (2000). IC identification circuit using device mismatch. Digest of Technical Papers - IEEE International Solid-State Circuits Conference, , 372-373. doi:10.1109/ISSCC.2000.839821
12. Zhang, X., Tuzzio, N., & Tehranipoor, M. (2012). Identification of recovered ICs using fingerprints from a light-weight on-chip sensor. Paper presented at the Proceedings - Design Automation Conference, 703-708. doi:10.1145/2228360.2228486 Retrieved from www.scopus.com
13. Ma, C., Zhang, S. -., & Chen, Z. (2016). Identification on counterfeit plastic encapsulated microcircuits. Paper presented at the Conference Proceedings of the 4th International Symposium on Project Management, ISPM 2016, 451-456. Retrieved from www.scopus.com
14. Wang, Y. L., Kuang, X., Huang, C., & Li, S. P. (2013). Case studied of failure threat caused by counterfeit plastic encapsulated microcircuits. Paper presented at the Proceedings of the International Symposium on the Physical and Failure Analysis of Integrated Circuits, IPFA, 574-577. doi:10.1109/IPFA.2013.6599226 Retrieved from www.scopus.com
15. Chang, H., & Sapatnekar, S. S. (2005). Full-chip analysis of leakage power under process variations, including spatial correlations. Paper presented at the Proceedings - Design Automation Conference, 523-528. Retrieved from www.scopus.com
16. Meshel, D. C., Harper, T., & Stradley, J. (2007). Preventing counterfeit parts and materials from the development of US national security space systems. Paper presented at the A Collection of Technical Papers - AIAA Space 2007 Conference, 3 2262-2274. Retrieved from www.scopus.com
17. Никифоров А.Ю., Скоробогатов П.К., Телец В.А. Идентификация изделий микроэлектроники и полупроводниковых приборов по радиационному отклику//Электроника, микро-и наноэлектроника. 2006. С. 140-144.
18. Давыдов Г.Г., Ожегин Ю. А., Телец В. А. Методика оперативной радиационной идентификации подлинности и соответствия заявленному типу изделий микроэлектроники//Стойкость. 2014. С. 15-17.
19. Bobrovsky D.V., Pechenkin A. A., Novikov A.A., Chumakov A. I., Ryasnoy N.V., and Churilin Y.V., “Flip-chip ICs SEE testing technique,” in Proc. 30th Int. Conf. on Microelectronics, MIEL 2017; Nis, Serbia, October 2017, pp. 309-311.
20. Demidova A.V., Pechenkin A. A., Borisov A. Y., Kessarinskiy L. N., Yanenko A. V., Boychenko D.V., and Nikiforov A.Y., “Different chips at identical marking on the example of OP1177,” in Proc. 14 th European Conf. on Radiation and its Effects on Components and Systems, RADECS-2015, Moscow; Russian Federation; Sept. 14 -18, 2015, article number 7365600.
21. Grebenkina A. V., Kessarinskiy L. N., and Boychenko D.V., “Analysis of radiation behavior of characteristics of precision rf passive components”, in Proc. 24th Int. Crimean Conf. Microwave and Telecommunication Technology, CriMiCo 2014, Sevastopol, Crimea, Ukraine, Sept. 07 - 13, 2014, pp. 872-873.

REFERENCES:

[1] KASPERSKY, E. V.. AUTOMATION HOSTAGE: HOW TO PROTECT THE INDUSTRY AGAINTS CYBER ATTACKS. IT Security (Russia), [S.l.], v. 23, n. 3, p. 7-10, oct. 2016. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/12>. Date accessed: 11 july 2018. (in Russian).
[2] ASTIER, Jean Yves; ZHUKOV, Igor Yurievich; MURASHOV, Oleg Nikolaevich. Smart Building Management Systems and Internet of Things. IT Security (Russia), [S.l.], v. 24, n. 3, p. 18-29, july 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/260>. Date accessed: 11 july 2018. doi:http://dx.doi.org/10.26583/bit.2017.3.02.
[3] EGOROV, Boris Mikhailovich et al. Main Directions in Ensuring Business Continuity for Information and Telecommunication Systems of High Availability. IT Security (Russia), [S.l.], v. 21, n. 4, dec. 2014. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/137>. Date accessed: 11 july 2018. (in Russian).
[4] Koushanfar, F., Fazzari, S., McCants, C., Bryson, W., Sale, M., Song, P., & Potkonjak, M. (2012). Can EDA combat the rise of electronic counterfeiting? Paper presented at the Proceedings - Design Automation Conference, 133-138. doi:10.1145/2228360.2228386 Retrieved from www.scopus.com
[5] Alkabani, Y., Koushanfar, F., Kiyavash, N., & Potkonjak, M. (2008). Trusted integrated circuits: A nondestructive hidden characteristics extraction approach doi:10.1007/978-3-540-88961-8-8 Retrieved from www.scopus.com
[6] Gassend, B., Lim, D., Clarke, D., Van Dijk, M., & Devadas, S. (2004). Identification and authentication of integrated circuits. Concurrency Computation Practice and Experience, 16(11), 1077-1098. doi:10.1002/cpe.805
[7] Nikiforov, A. Yu., Development of basic technology forecasting, assessment and control of radiation resistance of microelectronic products/Nikiforov A. Y., Skorobogatov, P. K., Strikhanov M. N., Telets V. A., Chumakov A. I. news of higher educational institutions. Electronics, 2012. - No. 5 (97). - P. 18-23. (in Russian).

[8] Pope, S. (2008). Trusted integrated circuit strategy. IEEE Transactions on Components and Packaging Technologies, 31(1), 230-234. doi:10.1109/TCAPT.2008.918319

[9] Origin Yu. a., Nikiforov A. Yu, Telets V. A., Uvarkin D. S., Pykhtina S. A. directions of development of quality management system for radiation tests the electronic component base. Special equipment and communication. 2011. No. 4-5. P. 59-62. (in Russian).

[10] Nikiforov A. Yu., Telets V. A. Radiation resistance of electronic component base of special equipment and communication systems. Spetstekhnika I Svyaz, issue № 4-5, 2011. (in Russian).

[11] Lofstrom, K., Daasch, W. R., & Taylor, D. (2000). IC identification circuit using device mismatch. Digest of Technical Papers - IEEE International Solid-State Circuits Conference, , 372-373. doi:10.1109/ISSCC.2000.839821

[12] Zhang, X., Tuzzio, N., & Tehranipoor, M. (2012). Identification of recovered ICs using fingerprints from a light-weight on-chip sensor. Paper presented at the Proceedings - Design Automation Conference, 703-708. doi:10.1145/2228360.2228486 Retrieved from www.scopus.com

[13] Ma, C., Zhang, S. -., & Chen, Z. (2016). Identification on counterfeit plastic encapsulated microcircuits. Paper presented at the Conference Proceedings of the 4th International Symposium on Project Management, ISPM 2016, 451-456. Retrieved from www.scopus.com

[14] Wang, Y. L., Kuang, X., Huang, C., & Li, S. P. (2013). Case studied of failure threat caused by counterfeit plastic encapsulated microcircuits. Paper presented at the Proceedings of the International Symposium on the Physical and Failure Analysis of Integrated Circuits, IPFA, 574-577. doi:10.1109/IPFA.2013.6599226 Retrieved from www.scopus.com

[15] Chang, H., & Sapatnekar, S. S. (2005). Full-chip analysis of leakage power under process variations, including spatial correlations. Paper presented at the Proceedings - Design Automation Conference, 523-528. Retrieved from www.scopus.com

[16] Meshel, D. C., Harper, T., & Stradley, J. (2007). Preventing counterfeit parts and materials from the development of US national security space systems. Paper presented at the A Collection of Technical Papers - AIAA Space 2007 Conference, 3 2262-2274. Retrieved from www.scopus.com

[17] Nikiforov A. Yu., Skorobogatov P. K., Taurus V. A. Identification of products of microelectronics and semiconductor devices on radiation response, electronics, micro-and nanoelectronics. 2006. P. 140-144. (in Russian).

[18] Davydov, Yu. a. Origina, Telets, V. A., Methods of operative radiological identification of authenticity and the compliance of the claimed type of microelectronic devices. Durability. 2014. C. 15(in Russian).

[19] Bobrovsky D.V., Pechenkin A. A., Novikov A.A., Chumakov A. I., Ryasnoy N.V., and Churilin Y.V., "Flip-chip ICs SEE testing technique," in Proc. 30th Int. Conf. on Microelectronics, MIEL 2017; Nis, Serbia, October 2017, pp. 309-311.

[20] Demidova A.V., Pechenkin A. A., Borisov A. Y., Kessarinskiy L. N., Yanenko A. V., Boychenko D.V., and Nikiforov A.Y., "Different chips at identical marking on the example of OP1177," in Proc. 14 th European Conf. on Radiation and its Effects on Components and Systems, RADECS-2015, Moscow; Russian Federation; Sept. 14 -18, 2015, article number 7365600.

[21] Grebenkina A. V., Kessarinskiy L. N., and Boychenko D.V., "Analysis of radiation behavior of characteristics of precision rf passive components", in Proc. 24th Int. Crimean Conf. Microwave and Telecommunication Technology, CriMiCo 2014, Sevastopol, Crimea, Ukraine, Sept. 07 - 13, 2014, pp. 872-873.

Поступила в редакцию - 20 апреля 2018 г. Окончательный вариант – 23 августа 2018 г.
Received – April 20, 2018. The final version – August 23, 2018.